

PKI SYSTEM

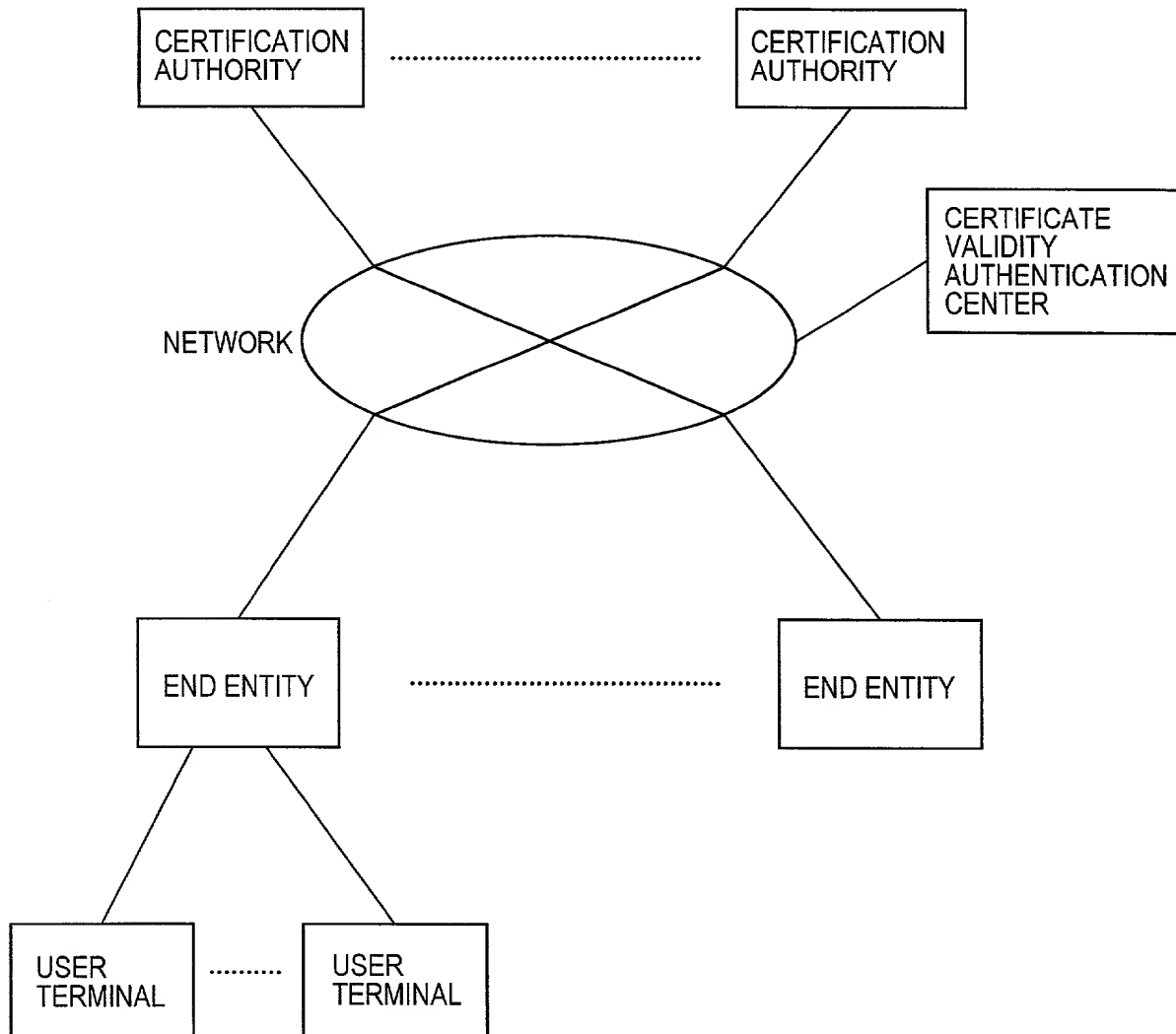
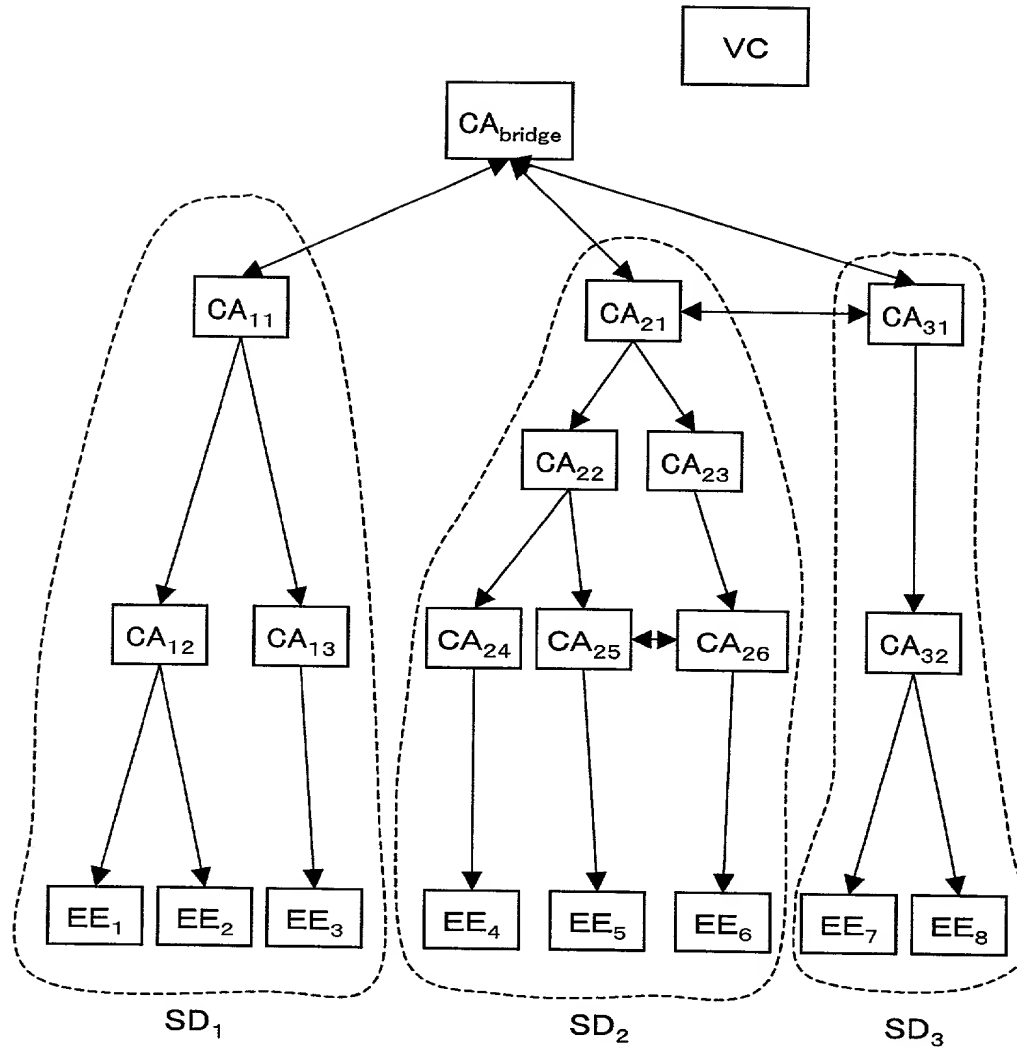


FIG.2



→ : FLOW OF PUBLIC KEY CERTIFICATE

CA : CERTIFICATION AUTHORITY

EE : END ENTITY

VC : CERTIFICATE VALIDITY AUTHENTICATION CENTER

SD : SECURITY DOMAIN

FIG.3

END ENTITY

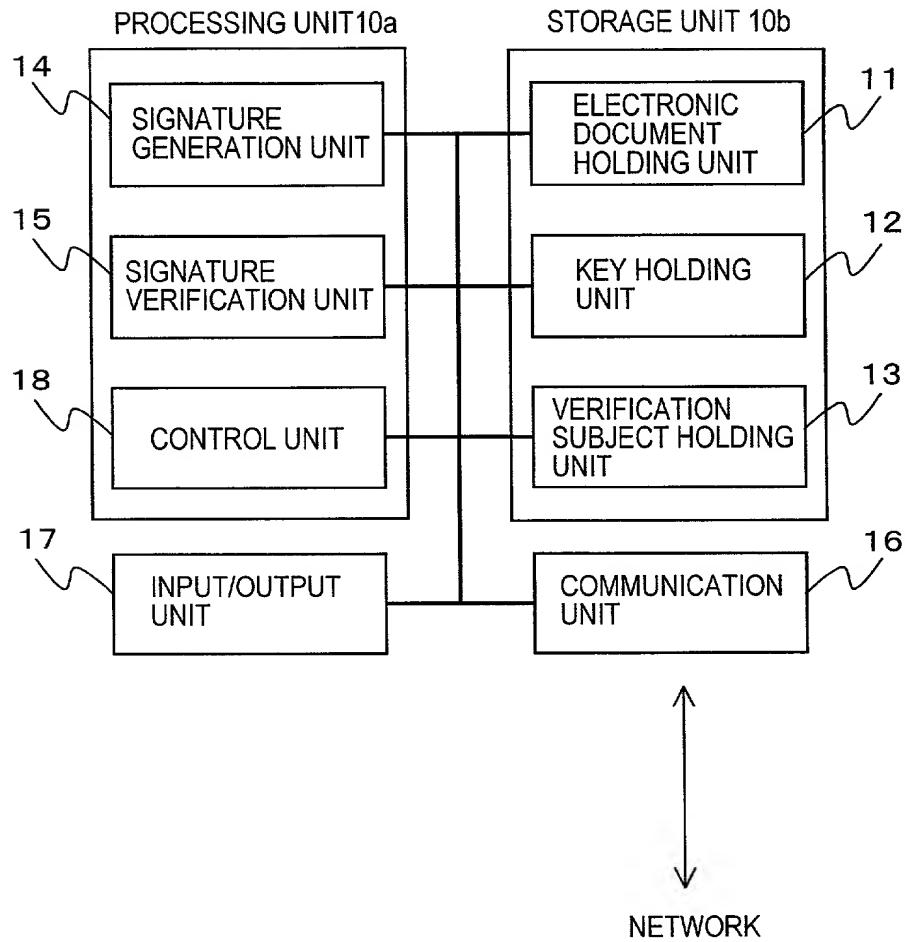


FIG.4

CERTIFICATION AUTHORITY

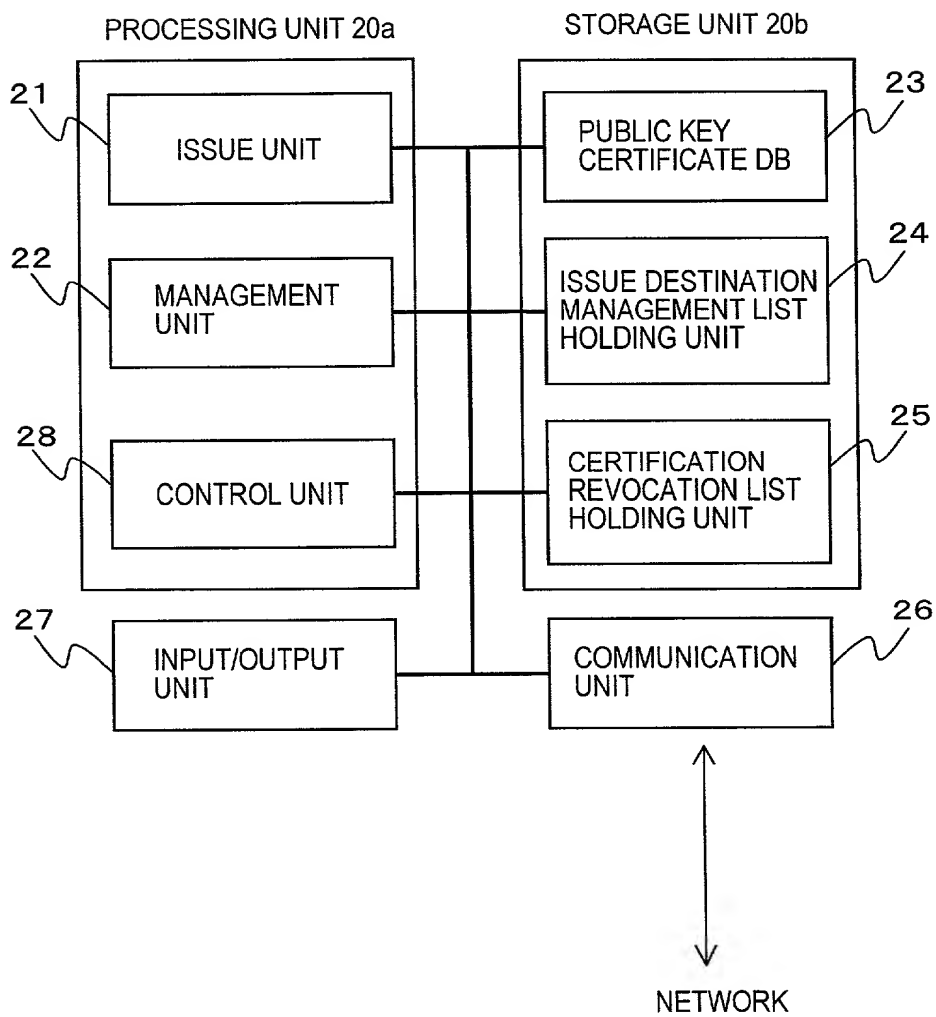


FIG.5

CERTIFICATE VALIDITY AUTHENTICATION CENTER

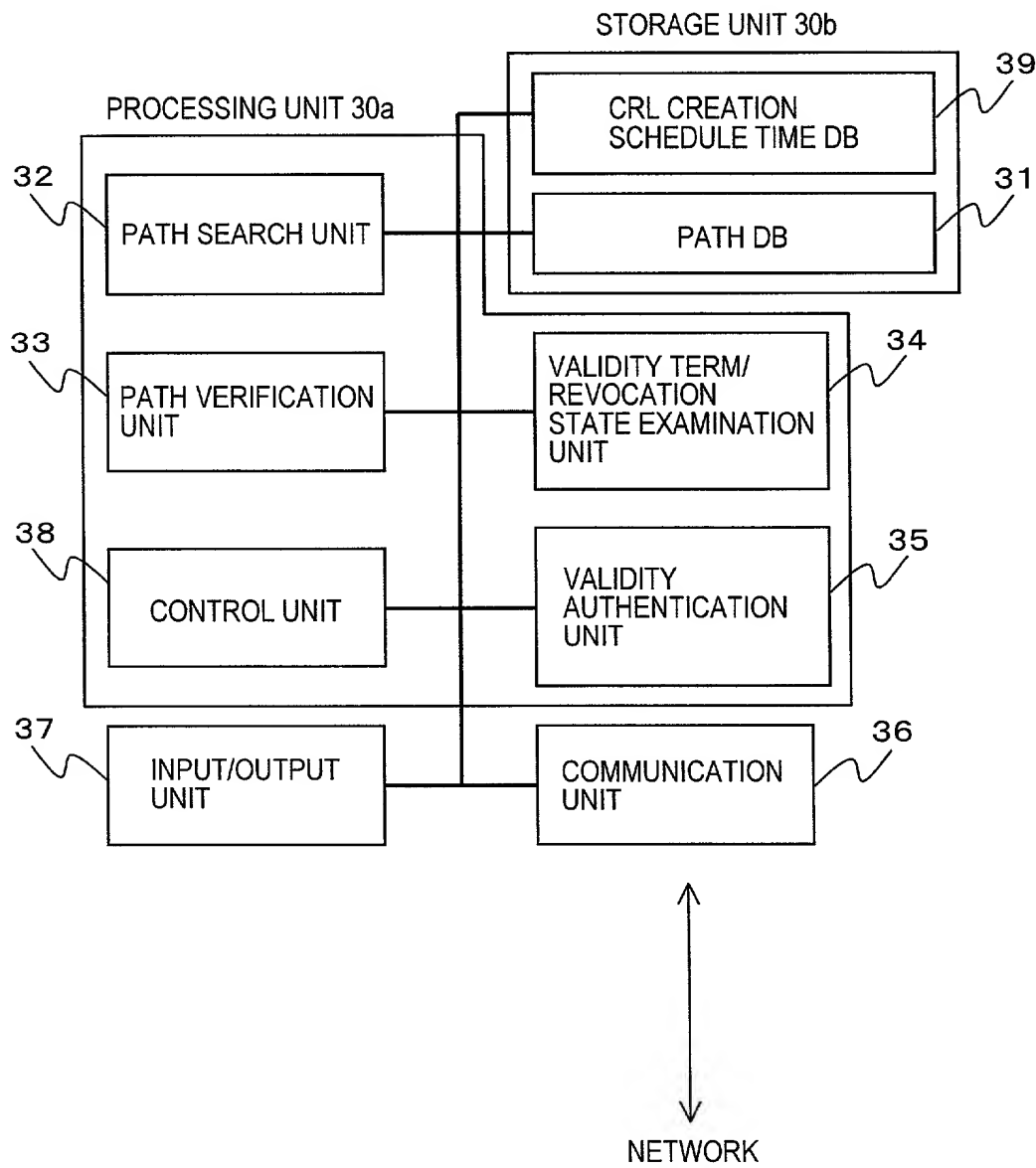


FIG.6

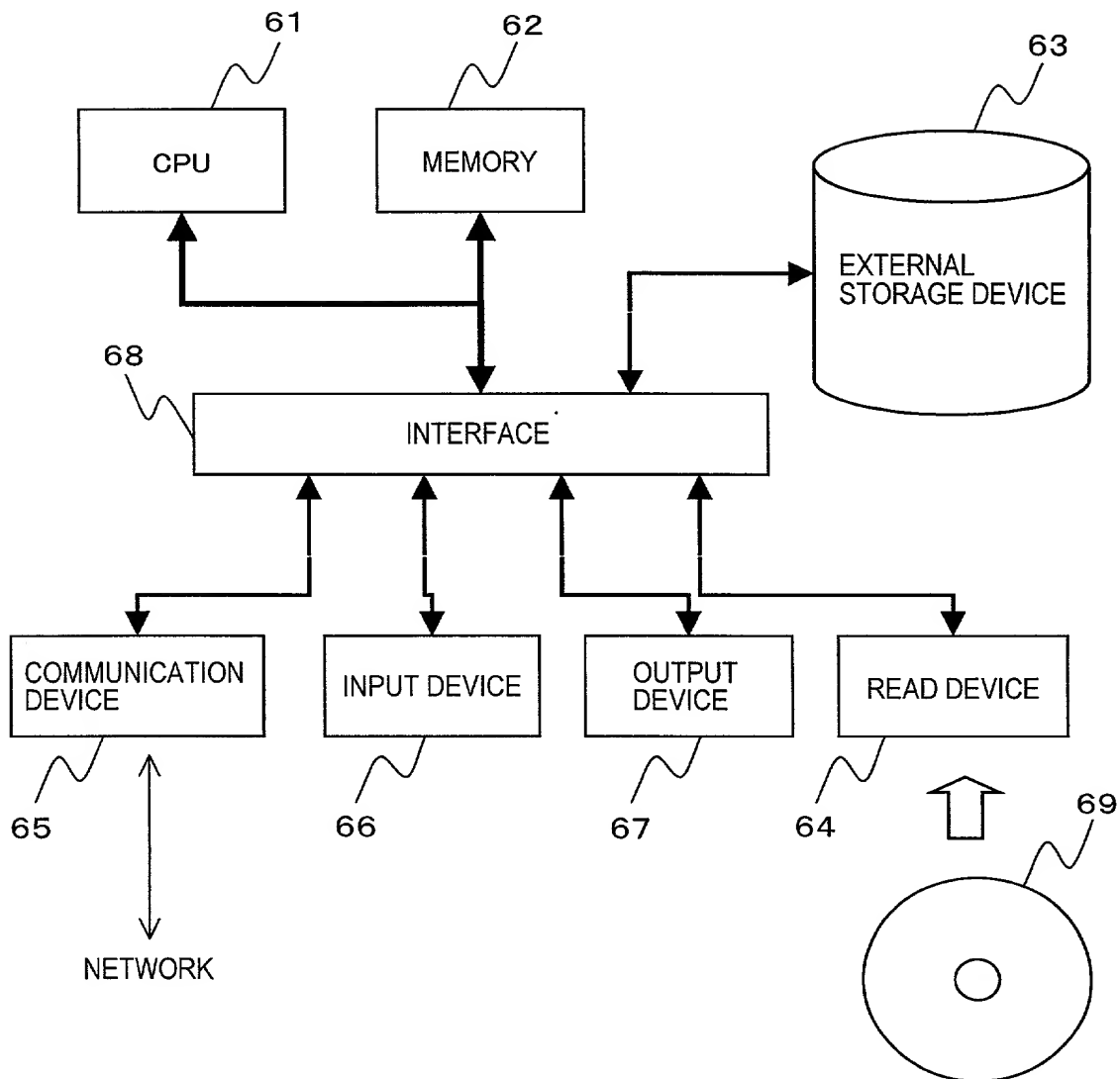


FIG.7

OPERATION OF SEARCHING FOR, VERIFYING AND MANAGING PATHS

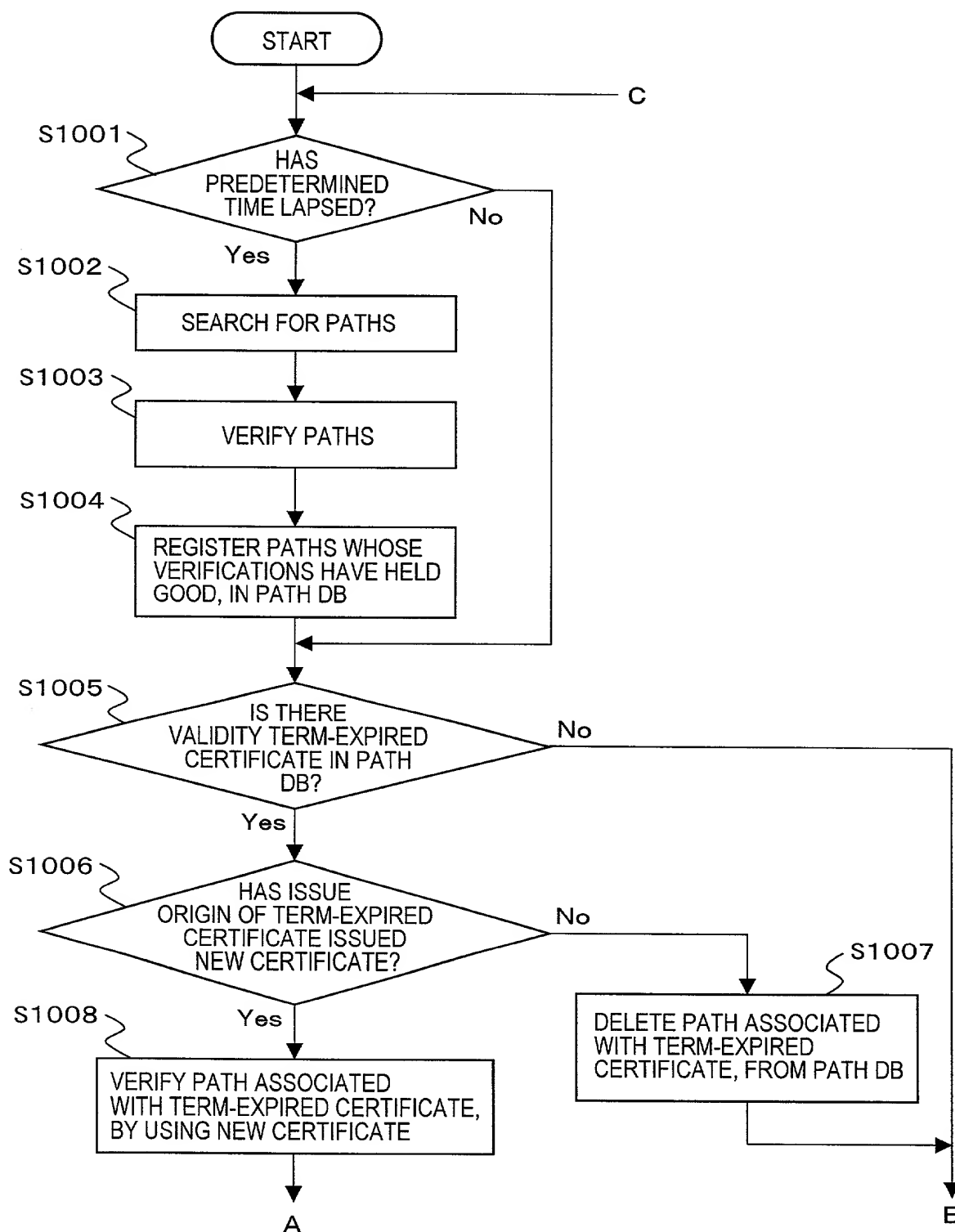


FIG.8

OPERATION OF SEARCHING FOR, VERIFYING AND MANAGING PATHS

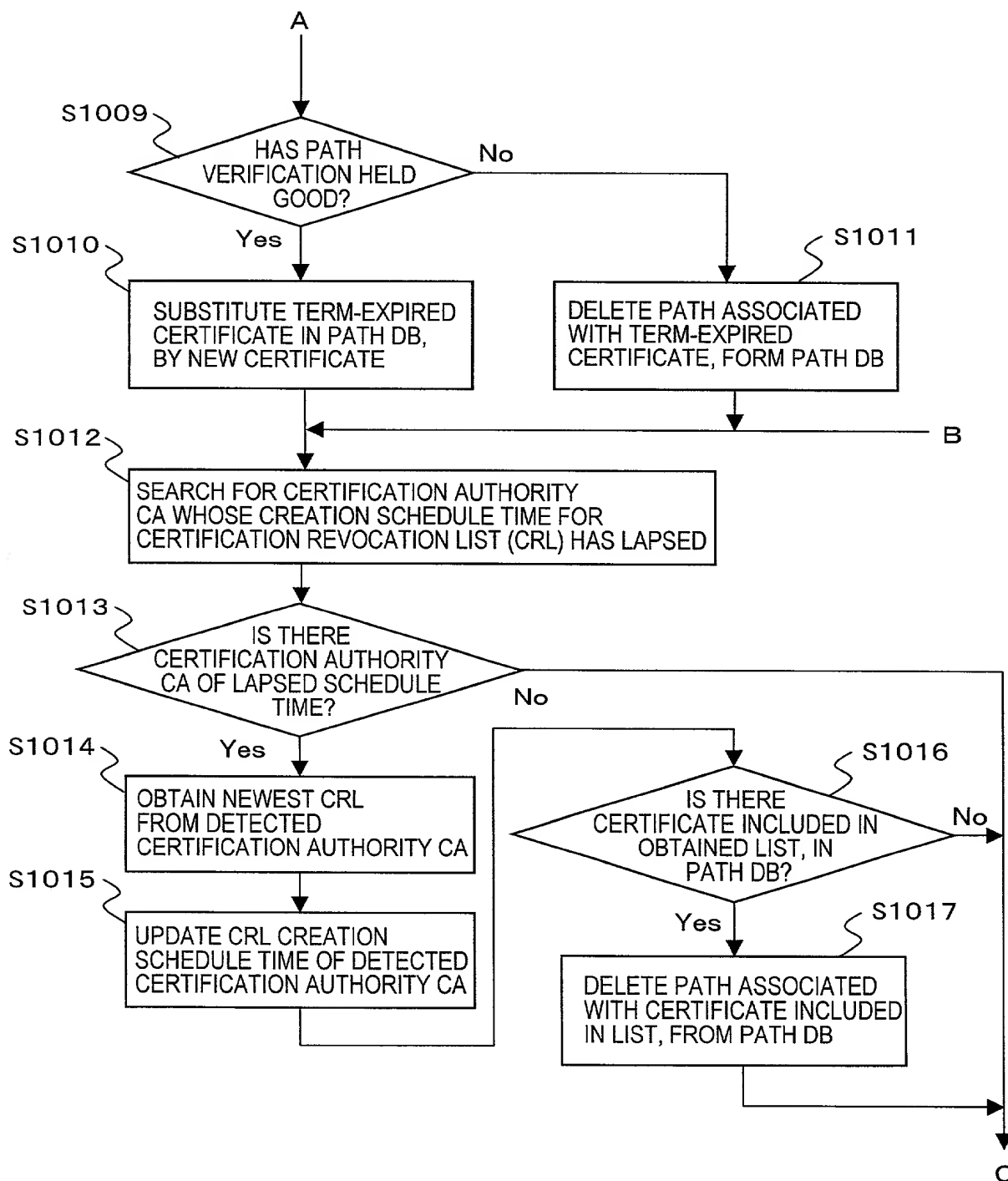


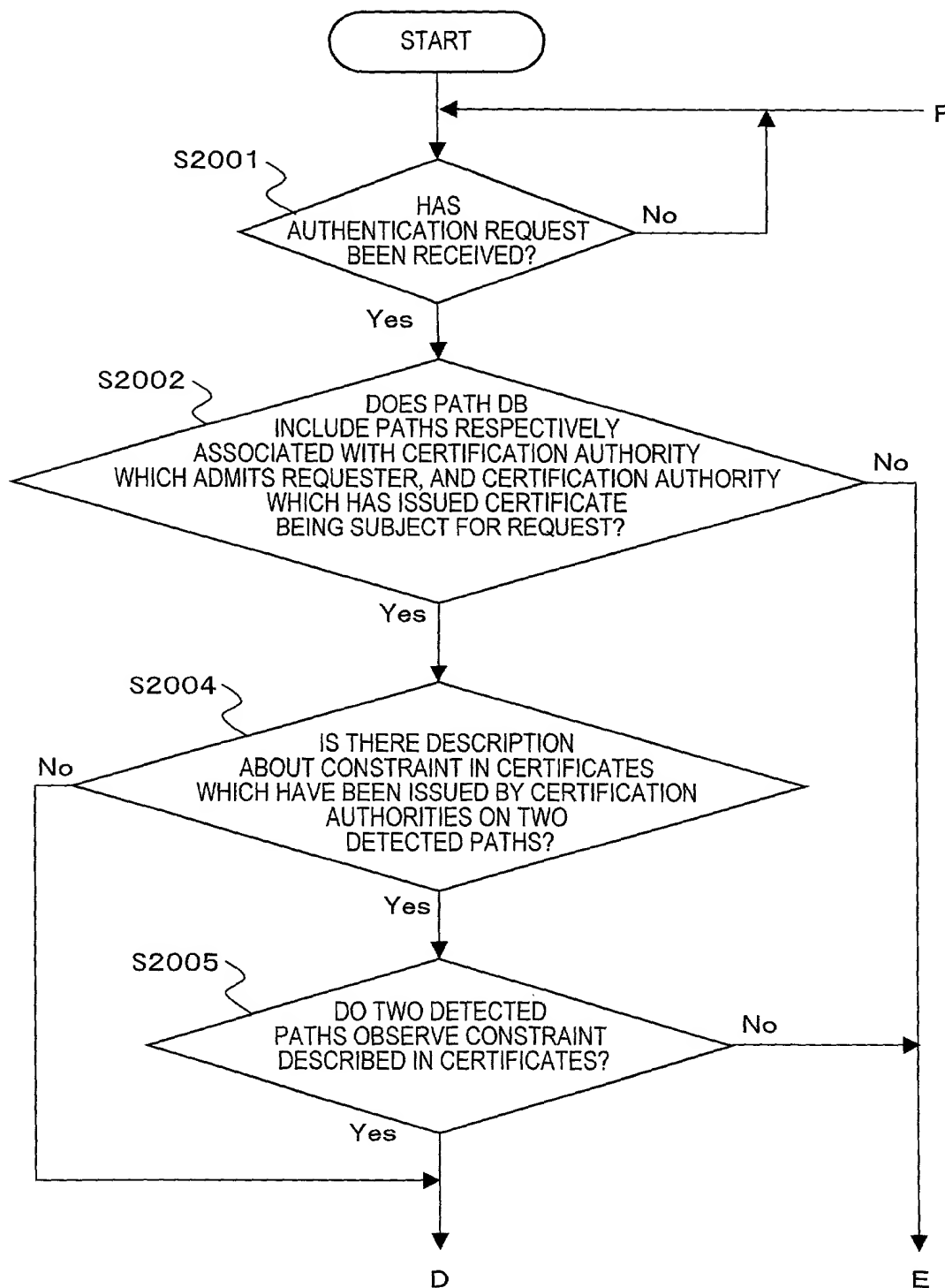
FIG.9

PATH SEARCH RESULT (IN CASE OF FIG. 2)

TERMINAL ADMITTING CERTIFICATION AUTHORITY	PATH
CA_{12}	$CA_{\text{bride}}-CA_{11}-CA_{12}$
CA_{13}	$CA_{\text{bride}}-CA_{11}-CA_{13}$
CA_{24}	$CA_{\text{bride}}-CA_{21}-CA_{22}-CA_{24}$
	$CA_{\text{bride}}-CA_{31}-CA_{21}-CA_{22}-CA_{24}$
CA_{25}	$CA_{\text{bride}}-CA_{21}-CA_{22}-CA_{25}$
	$CA_{\text{bride}}-CA_{21}-CA_{23}-CA_{26}-CA_{25}$
	$CA_{\text{bride}}-CA_{31}-CA_{21}-CA_{22}-CA_{25}$
	$CA_{\text{bride}}-CA_{31}-CA_{21}-CA_{23}-CA_{26}-CA_{25}$
CA_{26}	$CA_{\text{bride}}-CA_{21}-CA_{23}-CA_{26}$
	$CA_{\text{bride}}-CA_{21}-CA_{22}-CA_{25}-CA_{26}$
	$CA_{\text{bride}}-CA_{31}-CA_{21}-CA_{23}-CA_{26}$
	$CA_{\text{bride}}-CA_{31}-CA_{21}-CA_{22}-CA_{25}-CA_{26}$
CA_{32}	$CA_{\text{bride}}-CA_{31}-CA_{32}$
	$CA_{\text{bride}}-CA_{21}-CA_{31}-CA_{32}$

FIG.10

OPERATION OF AUTHENTICATING VALIDITY OF PUBLIC KEY CERTIFICATE



OPERATION OF AUTHENTICATING VALIDITY OF PUBLIC KEY CERTIFICATE

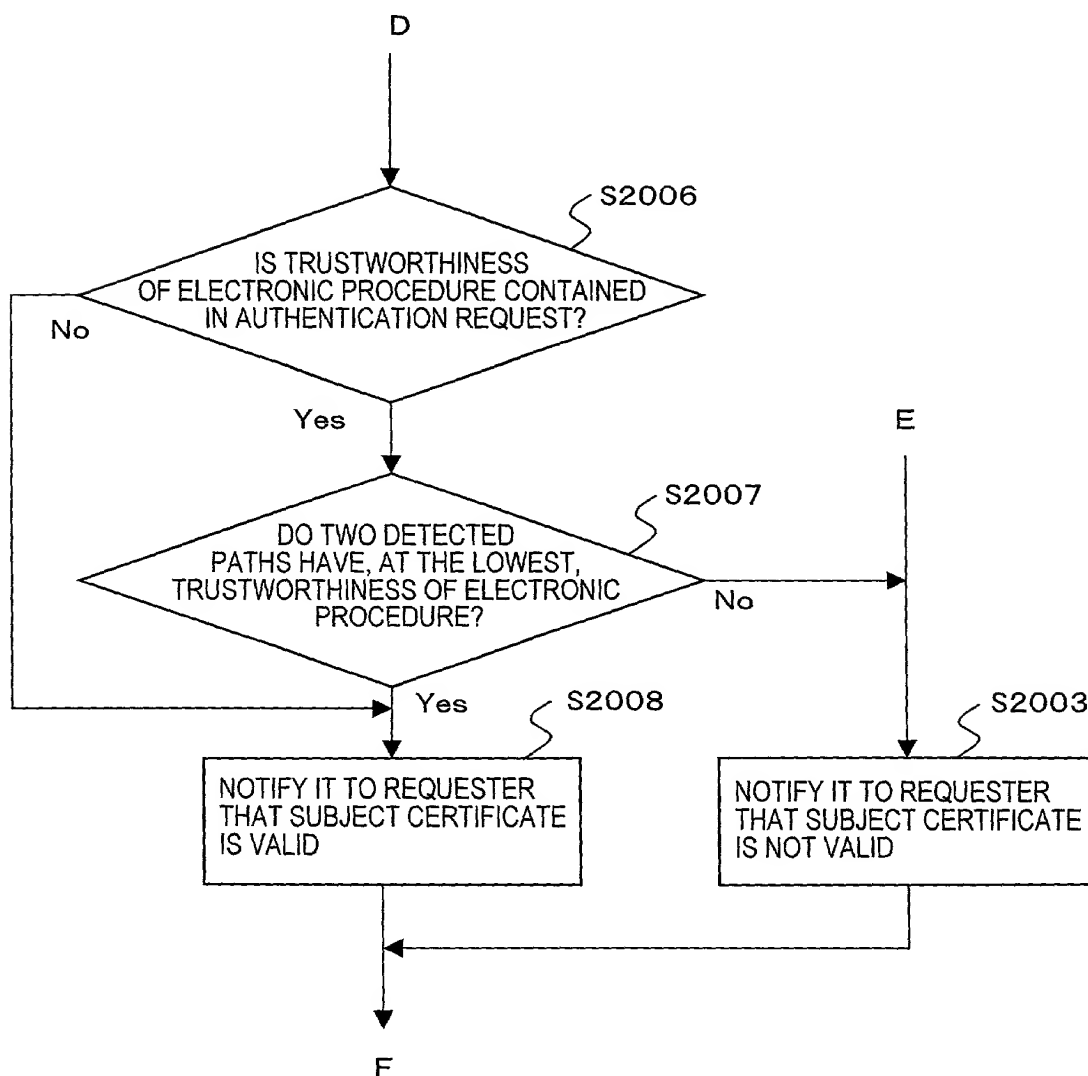
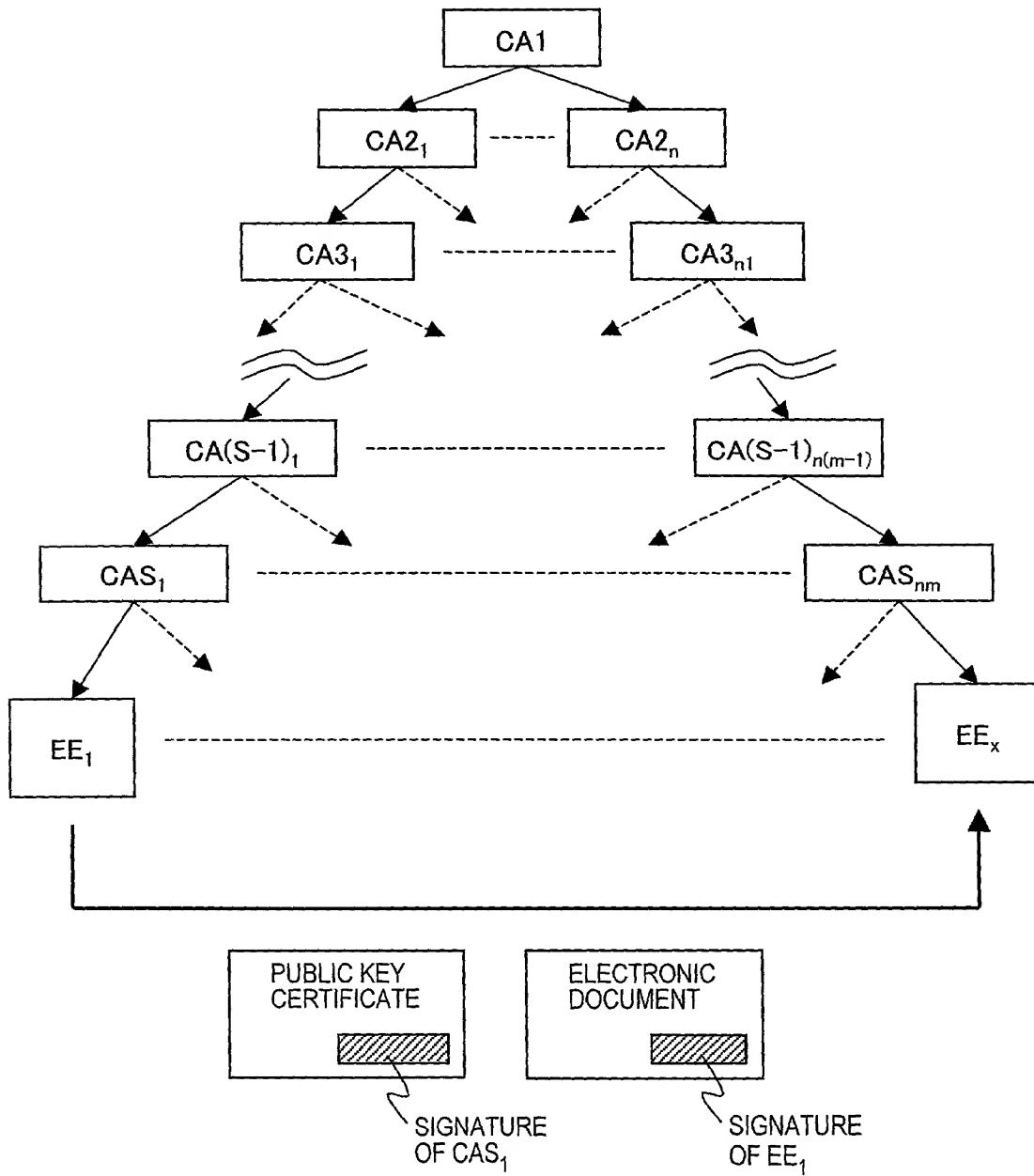


FIG.12



CA : CERTIFICATION AUTHORITY

EE : END ENTITY

—> : FLOW OF PUBLIC KEY CERTIFICATE